

NEWSLETTER

Volumen 7 · Issue 1 · Mexico City · February 2024



GPA

Global Privacy Assembly

PAGE 6

The Voice (Working Groups Highlights)

The outstanding importance of the GPA Resolution on Generative Artificial Intelligence Systems



PAGE 4

Horizon Scanning

Human rights impact assessments a useful tool into privacy trends



PAGE 15

Regional Perspectives

Cannon-Shot Rule for Data



PAGE 17

Meet our new members

Authority of Brazil, Nigeria and Niger



3

Message from the Chair

4

Horizon Scanning

Human rights impact assessments a useful tool into privacy trends.

6

The Voice (Working Groups Highlights)

The outstanding importance of the GPA Resolution on Generative Artificial Intelligence Systems.

7

In Conversation with

Data protection and environmental protection in the field of digital technologies: allies or foes?

9

Case Study

Indigenous perspectives on data privacy: Māori in Aotearoa New Zealand.

14

Get to know your ExCo

The Bulgarian Commission for Personal Data Protection. Strategies of the CPDP for the new challenges over personal data protection and the emerging technologies.

15

Regional Perspectives

Cannon-Shot Rule for Data- When someone uses data, whose interest does it serve? Whose should it serve?

17

Meet our new members

Authority of Brazil, Nigeria and Niger.

19

GPA highlights

An overall of the meeting outcomes.

Message from the Chair



President Commissioner: Adrián Alcalá Méndez



Commissioner: Josefina Román Vergara



Commissioner: Blanca Lilia Ibarra Cadena



Commissioner: Julieta Del Río Venegas

We stand at an essential moment in human history, where the new technologies have grown exponentially, the lines between reality and the creations of artificial intelligence (AI) begin to blur while the advances in neurotechnology spring up from dystopian imagination to concrete facts. In this matter, the GPA in Bermuda provided a platform for data protection authorities to raise their concerns and exchange best practices in addressing these challenges. The resolutions adopted and discussions held serve as a valuable roadmap for international cooperation and the development of stronger privacy frameworks in this new technological era.

The GPA in Bermuda has emphasized the role of civil society organizations and the private sector in promoting responsible technology development and advocating for individual privacy rights. The need for public awareness and education on data privacy issues was highlighted as crucial for empowering individuals to protect their rights and make informed choices.

One of the most important resolutions relayed on the Generative AI Systems; a document that seeks to guide us through this labyrinth of technological marvels and potential pitfalls. At its core, the resolution recognizes the immense potential of generative AI. This technology can craft art, compose music, generate text, and even forge synthetic faces. It boasts the power to revolutionize industries, fuel creativity, and enhance our lives in ways we can only begin to imagine.

However, with great power comes

great responsibility. All the work done during this meeting also warns us about the looming shadows of potential misuse of these advancements in technology capable of manipulating our own thoughts through neuroscience techniques. These technologies fueled by vast data sets, can churn out biased, discriminatory, or even harmful to citizens. This ability to manipulate reality at will by AI or to invade mind privacy in the case of neurotechnology, begs urgent questions about privacy, transparency, and accountability.

In the case of the privacy of the mind, it becomes an indispensable human right, perhaps the most important of all in a new era where the human mind can be undermined by the conflict of interests that these advances could lead to. The vulnerability of the individual in the free development of his personality, of his very essence as human, of free will, turns out disturbing.

It is urgent that these new technologies must first be regulated by ethics to which all science should be subject, as well as by projects of positive normativity and legal compliance that can be raised before legislative chambers across the world and of course, before international organizations with the power to show the rule of law. That is precisely one of the GPA goals, to ensure high standards of data protection globally and promote and facilitate effective regulatory cooperation on international perspectives.

The GPA in Bermuda undoubtedly maximized the organization's voice and influence and strengthened relationships with other international bodies and

networks such as the Future Privacy Forum, advancing data protection and privacy issues, including through outstanding arrangements. The international cooperation has been nourished with more members and new observers that enrich progressive, legal and morally committed activity of the Assembly vis-à-vis the population that each of our authorities represents.

The results gained over this meeting are not merely words on paper, but seeds sown for a future where privacy thrives alongside technological advancement. By addressing crucial issues like ethical AI, responsible data use in research, and global convergence in data protection, the GPA has taken concrete steps not only through the resolutions that came out of it in Bermuda but also by its Stra-

tegic Plan for 2023-2025, the Working Groups and the Joint Statements towards a world where individuals are empowered to control their data and innovation flourishes within a robust privacy framework. The journey to achieve these goals may be long, but the 45th GPA in Bermuda has set a clear direction, and the world now has a roadmap to follow. 🌐



Pam Dixon is the founder and executive director of the World Privacy Forum, a respected public interest research group. An author and researcher, she has written influential studies in the area of identity, AI, health, and complex data ecosystems and their governance for more than 20 years. Dixon has worked extensively on privacy and governance across multiple jurisdictions, including the US, India, Africa, Asia, the EU, and additional jurisdictions. Dixon currently serves as the co-chair of the UN Statistics Data Governance and Legal Frameworks working group, and is co-chair of WHO's Research, Academic, and Technical network. Dixon was part of the AI expert group that crafted the OECD AI Principles, which were ratified in 2019; she continues to work with the OECD and most recently was appointed to the AI Foresight Expert Group in 2023.

Horizon Scanning

Human rights impact assessments a useful tool into privacy trends

By Pam Dixon

Those working in the trenches of data protection and privacy are likely already aware that we have arrived at a major inflection point, one which promises to have meaningful impacts and even disruptions on privacy thought and practice. While privacy guardrails and normative AI principles are now in place across most jurisdictions, the intersection between established privacy thought and the shockwaves from advanced AI is like a chaotic, roiling sea that has yet to be fully tamed. How well privacy authorities navigate this difficult intersection will have significant influence on how privacy is articulated in AI and other data and information ecosystems for many years. A key advancement that data protection authorities can make is to create an expanded basis of analysis that will facilitate broader, long-term understanding of what is happening at the implementation levels of privacy and data.

As Global Privacy Assembly members will know, the **General Data Protection Regulation** has been adopted either directly or in near-identical legislation in most jurisdictions of the world. More than 164 jurisdictions and counting have some form of comprehensive data protection regulation in place today, making the GDPR model a meaningful guardrail which data protection authorities continue to work with. Add to this the newer set of multistakeholder AI principles and ethical AI principles, which were crafted largely from 2018 and through the pandemic at the OECD, UNESCO, WHO, and most recently, NIST. These normative AI principles and definitions of AI systems are already influencing recent legislative proposals such as the EU AI Act. The footprint of the GDPR and the new customary international law principles in AI are important safeguards in today's landscape. However, this landscape is shifting under our feet in near real-time.

Ready or not, a number of proposals have already been published that touch

on privacy as it is being interpreted in the current moment. Over 70 jurisdictions have a formal national AI strategy, most of which mention privacy. Some countries have already either passed or have started working on AI-focused legislation or guidance, for example, the EU AI Act, the US Executive Order on AI, and China's early AI regulations, among other examples. Although privacy is being mentioned in a lot of places, there is not yet a clear, normative articulation of what data governance, data protection, and privacy look like in advanced AI systems. Among the most important tasks data protection officials can undertake right now is to add more breadth, depth, and contextualization to traditional Privacy Impact Assessments (PIAs) by utilizing the expanded range of impact assessments that are now available. This is a key way that privacy experts can, over time, build a deeper basis of evidence regarding the governance of old and new data systems in their region.

A Human Rights Impact Assessment and Management Program (HRIAM) is a formal and extensively developed tool that is available for the purpose of broad and deep contextual analysis. It can go far to help DPAs and others integrate broader socio-technical analysis regarding data governance and protection. The UN Guide to Human Rights Impact Assessment and Management is the key frame of reference here, and this tool can be adapted per jurisdiction.

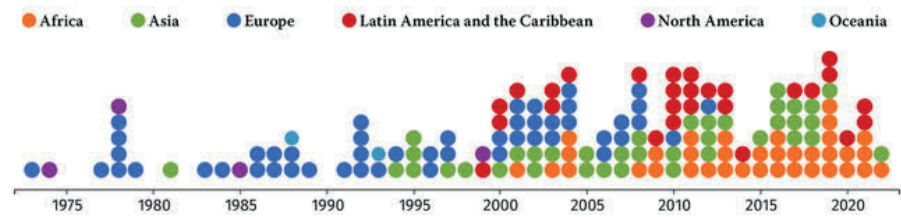


Image Source: World Privacy Forum. Research: Pam Dixon, Kate Kaye.
Data Visualization: John Emerson.

tion.¹ Working through a human rights impact assessment and management program (HRIAM) even for a small data system will facilitate the work of data protection offices to fully document and understand the judicial, economic, socio-technical, data, fairness, and other contextual aspects of the system being studied. Without a human rights impact assessment, what can happen is a sort of privacy “tunnel vision,” where new or emerging issues that may be outside of a DPA's traditional purview are not incorporated or mapped. For systems that are AI-specific or dominant, in addition to HRIAM, an AI-specific impact assessment and an ethical AI impact assessment are also helpful tools. There is already a large and detailed literature on HRIAM and both types of AI impact assessments.^{2 3}

The key benefit for DPAs in using tools such as HRIAM and AI impact assessments in addition to classical PIAs is that the more comprehensive data outputs from these tools allows DPAs to build an evaluative environment around data governance and privacy. This kind of measurement-rich environment that

measures far more than compliance numbers does not yet fully exist in privacy work today. There is a detailed discussion of the necessity of creating an evaluative environment in data governance, especially regarding AI systems, in a December 2023 WPF report, *Risky Analysis: Analyzing and improving AI Governance Tools*.⁴ The report discusses why evaluative environments for data governance are important, and how to start building processes to support such an environment.

The Ibrahim Index of African Governance,⁵ which comparatively analyzes human rights and other data across African countries over time, does a very good job measuring differences in contextual environments at the country level. This index requires data and many context-specific measurements. If there could be an Ibrahim Index for assessing privacy at depth and over time across use cases, data ecosystems, and country contexts, that would be ideal. To arrive at data-rich understandings, there has to be expert quantification of privacy across old and new data systems, and this effort could ideally be led by

¹ *Guide to Human Rights Impact Assessment and Management (HRIAM)*, United Nations, https://d306pr3pise04h.cloudfront.net/docs/issues_doc/human_rights/GuidetoHRIAM.pdf.

² *AI Impact Assessment definition*, NIST AI Risk Management Framework. <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>. See also: *UNESCO Ethical Impact Assessment*, UNESCO, 2021. <https://unesdoc.unesco.org/ark:/48223/pf0000386276>.

³ Some jurisdictions may also be very involved in the UN Sustainable Development Goals. If so, conducting an SDG Impact Assessment on data systems can be very helpful. See: *SDG Impact Assessment Tool*, United Nations. <https://sdgimpactassessmenttool.org/en-gb>.

⁴ Kate Kaye and Pam Dixon, *Risky Analysis: Assessing and improving AI Governance Tools*, World Privacy Forum. December 2023. <https://www.worldprivacyforum.org/2023/12/new-report-risky-analysis-assessing-and-improving-ai-governance-tools/>.

⁵ Ibrahim Index of African Governance, <https://mo.ibrahim.foundation/iiag>.



Data Protection Authorities, who are in position to test, measure, explore, study, understand, and articulate what privacy will mean in the rapidly changing and incredibly complex AI systems coming our way.

There is a lot to be learned. The older models of privacy governance offer us guidance, but they are incomplete

in ways that are not fully clear yet. We don't know all of the answers yet — we'll need to walk across the river by feeling the stones under our feet. These early steps can be made more sure by utilizing broader impact assessment tools that begin to capture more context, more breadth, and more depth of old and new parameters of privacy. 🌐

The Voice (Working Groups Highlights)

The outstanding importance of the GPA Resolution on Generative Artificial Intelligence Systems¹

By Wojciech Wiewiórowski, European Data Protection Supervisor



Artificial intelligence (AI) has undoubtedly emerged as a driving force transforming deeply the digital landscape. In this context, we certainly all recognise the potential of

generative AI to significantly affect our societies and share the concerns expressed in recent months regarding the ethical and legal implications of generative AI technologies, exacerbated by the release of generative AI systems to the public - often with insufficient pre-deployment assessment.

This is why we thought it was important to address the topic also at the global forum for data protection and privacy regulators that is the Global Privacy Assembly (GPA). It is indeed critical that GPA provides guidance to developers and users of these new technologies in a pro-active and timely fashion.

But I first would like to pay tribute to our colleagues from the Personal Information Protection Commission of Japan for putting the topic of generative



¹<https://globalprivacyassembly.org/wp-content/uploads/2023/10/5.-Resolution-on-Generative-AI-Systems-101023.pdf>

AI on the agenda of the G7 Roundtable of Data Protection Authorities that met in Tokyo in June 2023. Thanks to their leadership, the G7 DPA Roundtable adopted a statement on generative AI¹. The statement recalls specifically the need to continue this discussion in other international fora.

On that basis and with the support of G7 DPAs, the EDPS proposed to develop a GPA resolution on generative IA systems in the framework of the Ethics and Data Protection in AI Working Group that the EDPS has the honour to co-chair together with the CNIL. A drafting team worked tirelessly last summer under a very tight schedule to prepare the Resolution. I was impressed by the support received and immensely grateful for the work done. In particular, 19 authorities and institutions stood up to co-sponsor this Resolution which shows the relevance and importance of this initiative for GPA members.

Very importantly, this Resolution underlines that data protection and privacy principles and current laws, including data protection and privacy laws, bills, statutes and regulations, apply to generative AI products and services, even as different jurisdictions continue to develop AI-specific laws and policies.


It further endorses the existing data protection and privacy principles as core elements for the development, operation, and deployment of generative AI systems and provides initial guidance how these principles apply in this specific context.

These principles include the need for a lawful basis for the processing of personal data, purpose specification and use limitation, data minimisation, accuracy, transparency, security, privacy by design and by default, rights of data subjects, and accountability.

It is important to underline that, with the adoption of this Resolution, the GPA does not limit itself to restating these important principles, but makes a number of commitments to implement specific follow-up actions. In particular, GPA members commit to share ongoing developments within their jurisdictions within the Ethics and Data Protection in Artificial Intelligence Working Group and to coordinate their enforcement efforts on generative AI systems. In addition, GPA members consider

presenting, at the 46th GPA in Jersey, an interim report on the work conducted by the AIWG on generative AI systems, and finally consider additional policy documents or resolutions to be presented at the 47th Global Privacy Assembly that is scheduled to take place in Korea.

This Resolution is in my view one of the landmark resolutions of the GPA. With this Resolution, DPAs from all the world proved their capacity to coordinate in a very short timeframe on key messages on one of our most pressing challenges today and for the years to come. But this is only a first step and the work now has to continue. We look forward to engaging with our partners in the AI WG and all GPA members to ensure that the GPA is able to deliver on these important commitments.

By coordinating their efforts, DPAs from all over the world can indeed maximise their impact and play a strategic role to ensure that generative AI is integrated into day-to-day lives in a human-centred and sustainable way, respecting privacy and data protection principles. 

In conversation with

Data protection and environmental protection in the field of digital technologies: allies or foes?

By Camille Bourguignon

We are currently faced with two crucial phenomena: global warming (and the environmental transition) and the digital transition of our societies. The ability of digital technologies to better control and limit global warming has been for years actively highlighted by industrials and policymakers. For instance, the European Commission's Green Deal action plan promotes digital technologies - such as artificial intelligence, 5G, cloud and edge computing, Internet of Things, etc.- as being "critical enabler[s] for attaining the sustainability goals of the Green Deal in many different sectors"². However, digital technologies

are also depicted as one of the causes of the global environmental crisis. Their development in all sectors of society has worrying and growing negative effects on the environment.³ Contrary to the common belief that digital technologies would be "naturally green"⁴, they have a real footprint on the physical world.



Behind the screens, there are numerous data centers, networks, and devices.⁵ And behind all this, there is of course (without being exhaustive) corresponding energy consumption, carbon footprint, water consumption, biodiversity degradation and electronic waste.

The development of digital technologies is based on the use of more and more data, among which personal data. No viable artificial intelligence systems could indeed be developed without huge data sets at its basis. Products connected to the Internet - that are in-

cluded in what we call the Internet of Things ("IoT") - could not proliferate without the processing of large amounts of data all along the value chain.⁶ More broadly speaking, all our online activities could not take place without the collection and use of our data.

The use of data for developing digital technologies, as for any other activities, needs to comply with privacy and data protection laws. The application of data protection requirements influences the design of digital technologies. Therefore, it might have an indirect effect - positive or negative - on their environmental impact.

On the one hand, some principles stemming from data protection laws could be at odds with what the efficient environmental protection would normally require. Just think of the security measures required to comply with data security rules. Some of them are based on specific encryption techniques that require high computational resources (which have a huge negative environmental impact).⁷ Here, the application of data protection principles seems to worsen the negative environmental

² Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions – The European Green Deal, COM (2019) 640 final, 11 December 2019, p. 10.

³ See for instance LINC-CNIL, "Data, footprint and freedoms - Exploring the overlap between data protection, freedoms and the environment", IP Report, Innovation & Foresight, n° 9, available at https://linc.cnil.fr/sites/linc/files/2023-09/cnil_ip9_data_footprint_and_freedoms.pdf, June 2023, pp. 8 and f.; regarding the negative environmental impact of artificial intelligence precisely, see for instance M. HEIKKILÄ, « AI's carbon footprint is bigger than you think », MIT Technology Review, available at <https://www.technologyreview.com/2023/12/05/1084417/ais-carbon-footprint-is-bigger-than-you-think/>, 5 December 2023.

⁴ The negative environmental impacts of digital technologies, however, have been known since at least the early 2000s, see for instance F. BERKHOUT and J. HERTIN, "Impacts of Information and Communication Technologies on Environmental Sustainability: speculation and evidence", OECD Report, Brighton, University of Sussex, 25 May 2001, pp. 7-9. The words usually used to evoke digital technologies - "virtual", "cloud", etc.- contribute to vehiculate such a belief, see F. RODHAIN, *La nouvelle religion du numérique, Le numérique est-il écologique ?*, EMS Editions, Caen, 2019, pp. 28-41.

⁵ GreenIT.fr, *Empreinte environnementale du numérique mondial*, available at www.greenit.fr, October 2019.


⁶ The European institutions even call such products "data-driven technologies", see Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), O.J., L, 22 December 2023, recital 1.

⁷ R. CHATELIER, « Données et environnement : comment prévenir les marées noires du XXIème siècle », LINC- CNIL, available at <https://linc.cnil.fr/donnees-et-environnement-comment-prevenir-les-marees-noires-du-xxie-siecle>, 19 May 2021.

impact the technology concerned already has. A balance between data protection requirements and protection of the environment should then be found. It could be reached, for example, by using encryption techniques that require less computational resources. This would mean that the industry should create and offer “greener” encryption techniques and, if needed, first, should be prompted to do so. However, the efficiency of such an option is per se limited because at best it limits the negative impact, but it does not eliminate it.

On the other hand, other principles that govern the processing of personal data may indirectly help reduce the environmental footprint of some digital technologies. In particular, under the European General Data Protection Regulation (GDPR), controllers must define specified, explicit, and legitimate purposes for any processing of personal data. According to the ‘data minimization’ principle, controllers can process only data that are adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. They must also define the adequate duration for the storage of personal data.⁸ According to these rules, data protection requires ‘frugality’ in the processing of personal data. Logically, the less data is processed, the fewer computational resources and infrastructures are needed to make this processing, and the less negative environmental impact the data activity has.⁹ A frugality imposed in the use of data would even lead to sobriety in the use of the technology itself. For a concrete example, data protection principles can lead to limiting some practices, e.g. targeted advertising, that consu-

me huge amounts of data. Therefore, it would also lead to reducing the corresponding negative environmental impact of this activity. Here, even though they do not pursue the same objectives, data protection and environmental protection seem to converge.

The interactions between data protection and environmental protection require further and deeper analysis, which certainly needs to be done on a case-by-case basis. That said, because environmental degradation and climate change are not going to wait, the actors - including data protection authorities - should already integrate environmental considerations into their data protection practices.¹⁰ In this regard, the Global Privacy Assembly could be the right level to define guidelines and recommendations for such an integration. 



Camille Bourguignon

After practicing Law as a lawyer at the Paris Bar in the field of digital Laws for more than ten years, Camille recently decided to focus on the university activities she had in parallel. Camille now works as a lecturer and a researcher in digital technologies Law at the Center in Information, Law and Society (CRIDS-NaDi) and the University of Namur (Belgium). Her research activities focus on the links that must be made between the development of digital technologies and the fight against climate change and environmental degradation. With these issues in mind, Camille precisely began a doctoral program focusing on the question of the necessity to integrate the environmental concerns of digital technologies into the Law.

⁸ That said, for some data, the duration of storage can be regulated, even by data protection laws, and such imposed durations could per se have a negative environmental impact. Regarding in particular the obligation to store data for an appropriate duration to allow data subjects to exercise their right of access (the scope of which concerning not only the present but also the past), see C.J., case *College van burgemeester en wethouders van Rotterdam c. M.E.E. Rijkeboer*, 7 May 2009, C-553/07, EU:C:2008:773 commented by C. de TERWANGNE, “L’étendue dans le temps du droit d’accès aux informations sur les destinataires de données à caractère personnel”, R.D.T.I., 2011/2, n° 43, pp. 73-81.

⁹ A. N. BUDIYANO and J. KAO, “Data protection as part of an environmental, social and governance framework”, Bird & Bird, available at <https://www.twobirds.com/-/media/new-website-content/insights/pdfs/2022-personal-data-protection-digest-extract-jonathan-cao.pdf>, consulted on 18 January 2024, point 18.

¹⁰ For examples of possible ways for data protection authorities to integrate environmental dimensions into their recommendations or decisions, see LINC-CNIL, “Data, footprint and freedoms - Exploring the overlap between data protection, freedoms and the environment”, op. cit., pp. 63-64.

Indigenous perspectives on data privacy: Māori in Aotearoa New Zealand



By Tahu Kukutai, Professor at Te Ngira Institute for Population Research, The University of Waikato, Aotearoa New Zealand

Data privacy laws in most countries focus on the protection of personal data and personal data privacy. However, the Western emphasis on individualism contrasts with other traditions that see humans as relational beings whose identities and lifeways depend on their relationships with others and their environs. This relational paradigm – which is intrinsic to Indigenous cultures – has implications for how we think about data and data privacy.

In Aotearoa (New Zealand), our Indigenous-led research team has been developing a Māori data privacy framework as part of the 'Tikanga in Technology' (TiINT) programme funded by the Ministry of Business, Innovation and Employment. Aotearoa is an interesting case study, being both a founding mem-

ber of the DN network of the world's most digitally advanced nations and in the vanguard of the global Indigenous Data Sovereignty movement (Kukutai & Taylor, 2015). The Special rapporteur on the right to privacy has endorsed Indigenous data sovereignty in several reports (Cannataci, 2018, 2019), and called on governments and corporations to recognise the inherent sovereignty of Indigenous peoples over data about them or collected from them.

When our team began developing the Māori data privacy framework, we reviewed the literature to identify key features of an Indigenous approach to privacy (Kukutai et al., 2023). To summarise, we found:

- Indigenous concepts of privacy are inherently collective and are underpinned by Indigenous laws and protocols that determine when, how and by whom information and knowledge can or should be shared.

- Indigenous collectives assert that they have the right to own and control information collectively in much the same way that an individual owns and controls her personal information.

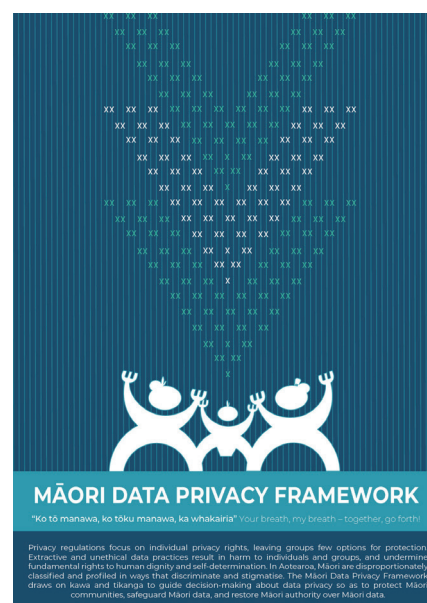
- Where an individual's information is intermingled with others – one obvious example being ancestry and genetic data – then there is a collective privacy right, and

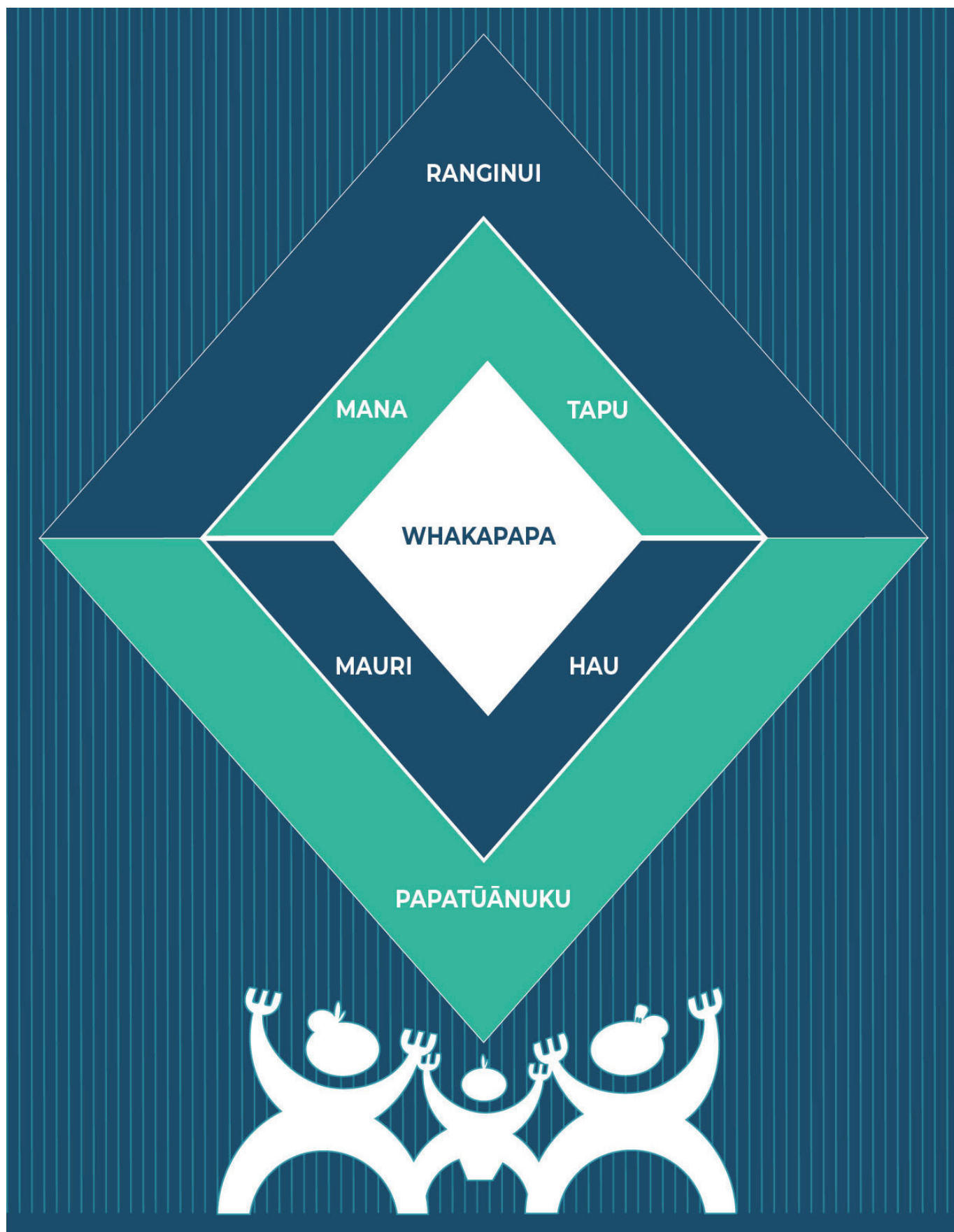
- Recognising and upholding relationships of belonging, responsibility and respect are paramount.

Clearly, for Indigenous peoples the protection of personal data is one part of a much wider set of data privacy considerations. In recent years Indigenous

groups have developed their own data protection technologies to try and give their communities some semblance of control over their information and to push back against well-documented practices of data colonialism (Couldry & Mejias, 2019; Mahelona et al., 2023).

Despite there being no word for privacy in the Māori language, there are well-defined cultural protocols or 'tikanga' that are central to a Māori concept of privacy. A 2016 paper by Māori law academic Khylee Quince explored how Western liberal notions of individualism and Māori collectivism produce very different cultural concepts of privacy, and how it is understood and applied. Our Māori data privacy framework extends her work in the specific context of data privacy and tries to offer some practical guidance. The core elements of the framework are shown below – the extended version has more detail.





ATUA

Ranginui and Papatūānuku protect the sanctity of our natural, social, and material worlds. Atua are our foundation, the ground truth, providing an enduring narrative of good spirit, connection and identity for current and future generations. Atua remind us that data and data technologies are human creations that entail responsibilities and accountabilities.

WHAKAPAPA

Whakapapa is the foundation of the Framework and recognises the reciprocal relationships between peoples, lands and waters. These relationships enable the intergenerational transmission of mātauranga, customs and protocols for what is right. Whakapapa situates data in a relational context. All data come from somewhere and someone. All individuals are part of a collective. Upholding whakapapa requires data privacy approaches that recognise and protect collective as well as personal privacy.

MAURI | LIFE FORCE

Mauri is the force of all life.

- Privacy law and standards will protect Māori data as a taonga.
- Māori data should be used in ways that enhance Māori wellbeing.
- Māori have the right to correct inaccurate or inappropriate data.

HAU | RECIPROCITY

Hau is the breath shared by all life forms. Hau gives effect to a moral code of reciprocity and accountability; therefore, a state of balance.

- Privacy law and standards shall protect the qualities of equity and justice.
- Free, prior, and informed consent is required for the collection and use of all Māori data including secondary use. Māori data governance is mandatory.
- Redress will be available for data breaches or misuse.

TAPU | PROTECTION

Tapu protects the sanctity of all life. In the context of data, tapu safeguards and upholds issues of data restrictions and sensitivity.

- Mātauranga Māori is a taonga that comes from and belongs to Te Ao Māori. Mātauranga, in all forms, must be protected and its transmission must remain with Māori.
- Māori will define what Māori data is open access.
- De-identified Māori data requires restrictions, given the greater risk of Māori being re-identified.
- Māori have the right to know if their data is being used to develop and/or train machines or algorithms, and have the right to opt out.
- Māori have the right to be free from data practices that are deceptive, manipulative, coercive, discriminatory or harmful.
- Storage, archiving and security protocols relating to Māori data will give effect to Māori data sovereignty. Māori owned and controlled infrastructure will be developed to ensure this level of protection.

MANA | AUTHORITY

To hold mana is to hold binding authority or power over one's domain including digital domains. Mana is held by individuals and groups.

- Māori will make decisions about how Māori data is collected, stored, accessed, deleted, shared and used, including secondary uses.
- Māori have the right to interpret, assess, interrogate and influence data practices and processes that affect them, and to halt them when necessary.
- A whakapapa approach to data privacy protects the rights of both individuals and collectives. In some contexts, collective Māori rights will prevail.

GLOSSARY

atua	gods	kawa	immutable protocols
mātauranga	Māori knowledges including science	Papatūānuku	earth mother
Ranginui	sky father	tikanga	values and practices for proper conduct
taonga	treasures, both tangible and intangible	whakapapa	genealogical relationships

CITE

Kukutai, T., Cairns, P., Cairns, T., Clark, T., Clark, V., Jacobs, R., Jones, N., Kani, H., Kepa, M., Kukutai, K., Morar, R., Muru-Lanning, M., Newbold, E., Port, W., Pouwhare, R., Rauwhero, B., Rauwhero, P., Shaw, R., Teague, V., Tuffery Huria, L., Watts, D. & Stirling, R. (2023). Māori data privacy framework (brief). Hamilton: The University of Waikato.

Ranginui — sky father - and Papatūānuku - earth mother - protect the sanctity of our natural, social and material worlds. Atua are our foundation, providing an enduring narrative of good spirit, connection and identity for current and future generations. Atua reminds us that data and data technologies are human creations that entail responsibilities and accountabilities.

Whakapapa is at the centre of the framework. Whakapapa is the genealogical layering and sequencing of relationships of all living things, from our founding ancestors to our digital versions of ourselves. All data comes from somewhere or someone.

Four tikanga values form the pillars of Māori data privacy.

The first is Mana. To hold mana is to hold binding authority or power over one's domain including digital domains. Mana can be held by individuals and groups. For Māori, having mana in a digital environment means that we should be able to make decisions about how our personal and collective data is collected, stored, accessed, deleted, shared and used, including secondary uses.

Tapu is an essential element of a Māori privacy concept. Tapu defines what is special or restricted. In the context of data, tapu safeguards and upholds issues of data restrictions and sensitivity. Genealogical and genetic data are considered tapu and have long been an area of concern for Māori (Law Commission, 2011). These concerns have been amplified by the proliferation of ancestry websites, Direct-to-Consumer genetic testing, the use of Forensic Investigative Genetic Genealogy (FIGG) by law enforcement agencies — including in Aotearoa- and the deployment of biometric technologies. The Privacy Commissioner recognises that Māori have significant concerns about the use of biometrics, especially the potential for bias and discrimination, and is consulting on new rules specifically for biometrics.

Mauri is the force of all life. Mauri requires privacy law and standards that protect Maori data as a taonga — a precious resource of tangible and intangible value. Where predictive analytics are used to classify and derive information about Māori, it must be regulated in ways that are consistent with tikanga.

Hau is the vital essence of life that is shared by all living things. In digital worlds, hau symbolises a state of balance based on a moral code of reciprocity. Hau requires privacy law and standards that protect the qualities of equity and justice, that uphold respectful relationships, and enable a range of options for redress when data breaches harm Māori, including tikanga options.

In developing the framework, the guidance of our TiNT kaumātua (elders) has been crucial. Their hope is for a privacy paradigm that protects all of the digital lives of their mokopuna (grandchildren) - one that is grounded in a more holistic and relational practice of informational self-determination than a narrow focus on individuals. 🌐

-
- Cannataci, J. (2018). *Big data and open data taskforce report (A/73/438, United Nations General Assembly)*. Available from: <https://www.ohchr.org/en/calls-for-input/reports/2018/report-bigdata-and-open-data>
 - Cannataci, J. (2019). *Report on the protection and use of health-related data (A/74/277, United Nations General Assembly)*. Available from: <https://www.ohchr.org/en/calls-forinput/reports/2019/report-thee-protection-and-use-health-related-data>
 - Carroll, S., Garba, I., Figueroa-Rodríguez, O. L., Holbrook, J., Lovett, R., Materechera, S., Parsons, M., Raseroka, K., Rodriguez-Lonebear, D., Rowe, R., Sara, R., Walker, J. D., Anderson, J., & Hudson, M. (2020). *The CARE principles for Indigenous data governance*. *Data Science Journal*, 19(43), 1–12. <http://doi.org/10.5334/dsj-2020-043>
 - Couldry, N., & Mejias, U. (2019). *The costs of connection: How data are colonizing human life and appropriating it for capitalism*. Stanford University Press.
 - Kukutai, T., Cassim, S., Clark, V., Jones, N., Mika, J., Morar, R., Muru-Lanning, M., Pouwhare, R., Teague, V., Tuffery Huria, L., Watts, D. & Sterling, R. 2023. *Māori data sovereignty and privacy. Tikanga in Technology discussion paper*. Hamilton: Te Ngira Institute for Population Research, The University of Waikato. https://tengira.waikato.ac.nz/_data/assets/pdf_file/0004/961645/MDSov-and-Privacy_20March2023_v2.pdf
 - Kukutai, T. & Taylor, J. (eds). 2016. *Indigenous data sovereignty: Toward an agenda*. Canberra: ANU Press.
 - Law Commission (2011). *Review of the Privacy Act: Review of the law of privacy, stage 4 (Report 123)*. <https://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20R123.pdf>
 - Mahelona, K., Leoni, G., Ducan, S. & Thompson, M. (2023). *Open AI's Whisper is another study in colonisation*. <https://blog.papareo.nz/whisper-is-another-case-study-in-colonisation/>
 - Quince, K. (2016). *Māori concepts in privacy*. In S. Penk & R. Tobin (Eds.), *Privacy law in New Zealand (2nd ed.)* (pp. 29–52). Thomson Reuters.

Get to know your ExCo: The Bulgarian Commission

Strategies of the CPDP for the new challenges over personal data protection and the emerging technologies.



Cathedral of St. Alexander Nevski in Sofia, Bulgaria/
by Tom Fournier

By Ventsislav Karadjov

The Commission for Personal Data Protection of the Republic of Bulgaria (CPDP) was established, just two decades ago, in 2002 with main power to guarantee the fundamental civil right to protection of natural persons' rights with regard to processing of their personal data. Our institutional vision is to build and develop a public environment in which the integrity of the individual and citizens' privacy are guaranteed through a system of prevention, accountability and control measures against the wrongful processing of personal data.

We are independent government authority ensuring individuals' protection

in the processing of their personal data and the access to these data and exercising control over the compliance with the General Data Protection Regulation (Regulation (EU) 2016/679) and Personal Data Protection Act of the Republic of Bulgaria, which incorporates the Law Enforcement Directive as part of the EU transposition process. The CPDP consists of a Chairman and 4 members. Currently, our team has 117 qualified experts which is a staff increase of 35% since last year while our annual budget as a first level spender has been almost doubled (87%).

After more than twenty years, based on our extensive expertise and admini-

nistrative capacity, Bulgarian National Assembly (as a supreme legislative authority), casts additional powers to us under the national transposition of the Whistleblowers Protection Directive of the European Union. Currently, the Bulgarian Commission is also the national central body for external secured signal reporting and for the protection of the persons, to whom such protection is provided in the sense of the Bulgarian Whistleblowers Protection Act.

The CPDP is one of the operative members of the European Data Protection Board. As a newly established EU institution in 2018, appointed Bulgarian representatives played role in strengthening its capacity building and international reputation. The CPDP Chairman was three terms Deputy Chair of the EDPB and its predecessor – the EU Article 29 Working Party for more than 9 years and he was involved actively in the establishment of the recently at that time developed body and its worldwide promotion. The 40th Global Privacy Assembly was conducted for the first time in two different venues by the CPDP and European institution in 2018 demonstrating not only the capacity for innovations but also capability to deal with challenges by using contemporary high-tech solutions.

This is just a couple of evidences for our international commitment. International cooperation is a matter of priority for the Bulgarian Commission for Personal Data Protection. During the last decade we built strong international team in the Commission full of experienced

and competent professionals who can dedicate their skill and efforts for achieving the objectives of the Global Privacy Assembly.

We consider that the world-wide-recognized Global Privacy Assembly has become the “Gold Standard” for international privacy protection, uniting more than 140 public and private bodies and organisations joining efforts in protecting human rights and dignity via ensuring high-level solutions for privacy and data protection. Current challenges in multidisciplinary areas such as neuroscience and artificial intelligence are just the peak of iceberg. They are trendy and attractive because of the fast development of the technologies nowadays, but they also demand deep understanding and independent supervision how this complex processing of personal data complies with worldwide-established standards for privacy from the very moment of their design.

More important and valuable one is



Ventsislav Karadjov — Chairman of the Bulgarian Commission for Personal Data Protection, 2014; two terms Vice-Chair of the EU Art. 29 Working Party, 2014- 2018; EDPB Deputy Chair, 2018-2023.

the everyday cooperation between all of us. It was sporadic and on annual basis several years ago and now it is every day routine work, responding to the global threats regardless of the geographic region or the maturity of the national system for personal data protection. Thus, we all together seek and contribute to the development of a worldwide privacy

environment in which the rights of individuals are guaranteed through mutual recognised systems of prevention, accountability and supervision.

As GPA Members, we all together should deepen local, regional and transnational cooperation between public institutions, academia, private sector and civil society organisations. 🌐



Regional Perspectives

A Cannon-Shot Rule for Data?

When someone uses data, whose interest does it serve? Whose should it serve?

By Alexander White, Bermuda Privacy Commissioner.

Often organisations have unbalanced incentives to use personal information solely for their own interest, to the detriment of individuals or even society as a whole. Much has been written about the surveillance economy and how organisations capitalise by measuring the online and real-world behaviours of individuals. We —all of us— are being

observed and quantified to new extremes, with both potential benefits and new potential for harm.

The use of observational insights is not a new phenomenon. The course of human progress has been built on the scientific method, which relies on observation and quantitative measurement —the measurement of reality

itself, the physical world, and certainly individual persons. Early agriculture meant noticing patterns of stars and the resulting changes in seasons— seeing the trend, and taking advantage of the pattern. Early healthcare started by noticing that when someone ate one thing they were ill — and then something else made them better.

Modern data protection laws give rights to individuals through a personal sovereignty or decision-making power regarding the various facts and statistics that refer to them. But, in giving individuals the protection of the state or a right of ownership over observations about themselves, are we in fact giving them a sovereignty over a slice of reality — or the ability to control how others may perceive the world? How far should that reach?

Analogies about data tend to refer to it as a resource for science or industry, such as oil or electricity. I find it useful to think of data in the analogy of shared spaces, as a “new commons” — with both the benefits and the tragedies that comparison implies. In many legal traditions, anyone in a community could potentially access or use a common resource, like grazing land, and no one can exclusively own it. This means that the resource could be abused in ways that harm specific people, because no

one has direct responsibility for it. This is yet another problem that exists today in the context of data.

In the past, we as a global society have had to come together and decide what should be a common resource, and what can legitimately be claimed by one party.

As we look out the windows here in Bermuda, we are struck by views of the sea. The oceans are a global resource for transportation, aquaculture, or other shared purposes. When faced with the question of how much of the ocean a country could claim, early modern nations judged that the distance a weapon could reach was a reasonable meas-

ure of control of a slice of the common seas. The distance that a cannonball could be fired from the coastline was about the distance to the horizon. Setting aside the merits, this consensus provided a clarity on the norms of one party's reach and allowed both sides to understand one another's expectations. As time passed and technology changed, the consensus definition for sovereign territory gradually expanded, until our global society reached a general agreement under the twentieth-century Law of the Sea.

Humans needed similar agreements when we began to regularly explore and inhabit new spaces, such as the only continent without an indigenous population, Antarctica. In that case, a treaty system helped established a consensus on expectations and norms for how the region may be used for scientific research purposes. Threats from militarization and zero-sum competition have been largely avoided to allow access and progress for the world to benefit from. In another instance, the Outer Space Treaty established an agreement that one group cannot claim ownership over celestial objects, and instead we should consider the use of these resour-

45th GLOBAL PRIVACY ASSEMBLY BERMUDA 2023



Ripples | Waves | Currents



Privacy Commissioner
Bermuda | Quo Data Ferunt

ces for all humankind.

We are fast approaching (if we have not already passed) the point where that conversation is needed in terms of data, algorithms, inferences, profiles, and other uses of observational technology. A claim of exclusive ownership or control limits the ability to use a resource for the common good — it limits the ability to benefit all humankind.

Unlike a commons, even specific data are usually reusable resources — they are not necessarily consumed when they are used. Therefore, there is the

potential that knowledge creation and research could continue to make use of personal information in a non-exclusive way that allows multiple parties, and even our communities as a whole, to benefit from the use.

But — that same personal data can also be reused infinitely for harm to individuals.

As representatives of the world's data protection authorities, we have a responsibility to lead the conversation. We must come together to decide how far the cannon shot of an individual's claim on personal information can reach. Is it time for a treaty system establishing conventions on data?

At the Global Privacy Assembly in Bermuda, where you are never far from shores and historic forts, I asked the question: Can there be a cannon-shot rule for data?

We should begin developing this international consensus. Let's start by asking: What do we agree on? How can we ensure that a potential use of personal information is trustworthy and fair — and how can we make sure that technologies serve all humankind? 🌐

Meet our new members 2023

BRAZIL

We are glad to welcome Brazil as a new member to the Global Privacy Assembly. A Autoridade Nacional de Proteção de Dados celebrated its third anniversary this November 2023. The ANPD has been proactive in enforcing the Lei Geral de Proteção de Dados Pessoais (LGPD), conducting inspections, investigating complaints, and imposing sanctions on non-compliant entities. This has sent a strong message to organizations that they need to comply with the law, and it has helped to raise awareness of data protection among the Brazilian public.

Moreover, the ANPD has been providing guidance and resources and collaborating

with stakeholders to foster a culture of data privacy. This has helped to empower individuals to understand their data protection rights and to hold organizations accountable for their data handling practices.

Brazil is undoubtedly a great reference in terms of personal data protection in the Americas and that is why the GPA is proud to count with them among its ranks. There is a bright future together on the way ahead.

The Presidency of the ANPD is held by the Director-President and is currently headed by Mr. Waldemar Gonçalves Ortunho Júnior.

NIGER

We also welcome Niger. La Haute Autorité Pour la Protection des Données à caractère Personnel (HAPDP) is the regulatory authority for personal data protection in Niger. It was established in 2017 through Law No. 2017-28, which was subsequently amended by Law No. 2019-71 in December 2019.

The HAPDP plays a crucial role in ensuring the protection of personal data of individuals in Niger. Its key responsibilities include:

- Ensuring compliance with data protection laws.
- Overseeing data transfers abroad, ensuring that such transfers are conducted in accordance with the law and that adequate safeguards are in place to protect individuals' privacy.
- Issuing guidelines and recommendations to data controllers and processors, helping them adhere to data protection standards and implement necessary measures to protect personal data.
- Investigating complaints related to data protection breaches and takes appropriate enforcement action against non-compliant entities, including imposing fines and issuing reprimands.
- Increasing data protection awareness through educational initiatives to pro-

mote data protection literacy among individuals and organizations in Niger, fostering a culture of responsible data handling.

After having a rough overview, and welcoming Niger, there is no doubt that we understand that the extraordinary effort and work of the HAPDP in the midst of the very difficult circumstances that Niger is currently experiencing deserves double recognition and our support so that the work of the HAPDP continues.

The Data Protection Authority of Niger is Ms. Sanady Tchimaden Hadatan, Grand-Croix dans l'ordre National.

NIGERIA

Another new member is Nigeria. The Nigeria Data Protection Commission (NDPC) is an independent agency tasked with safeguarding of personal data of Nigerian citizens. On June 12, 2023, a new Data Protection Bill was signed by President Bola Ahmed Tinubu.

This Act has distinctive mandates:

The Act launches a new category of "data controllers and processors of major importance," it is a reference to the EU's Digital Services Act and its specific obligations for "very large online platforms and search engines;"

A "duty of care" is a rule of compliance for controllers and processors of data.

Controllers and processors must seek the services of a data protection compliance organization (DPCO) to perform a data protection audit.

The Act has some remarkable extraterritorial canons.

The Act points out limitations on legitimate interest as a legal basis for personal data processing. That was not present in Nigeria's previous data protection laws.

The Act cares for children and other vulnerable people like those with no

legal capacity.

Finally, the Act delineated formal changes to the data protection authority, going from "Bureau" to a Commission, and modernized the governing mechanisms for the authority.

In conclusion, the NDPC has garnered praise for its efforts to be at the forefront of international standards in the protection of privacy and personal data rights. We are sure that their work in alliance with the GPA will build a better future in guaranteeing the Nigerian's privacy rights and to be a reference to follow on the African continent.

GPA highlights

An overall of the meeting outcomes.



The 45th Global Privacy Assembly took place in Hamilton, Bermuda, from October 15 to 20, 2023. The open session stood out for introducing innovative topics, such as the Privacy Law Developments in the Caribbean Community, Advancing Technological Policy, social harms that may arise with technology in privacy, such as Artificial Intelligence (AI), the intersection between Personal Data Protection and regulation in other areas like Competition and Consumer protection, safeguarding data in financial services in an era of global financial interconnectedness, quantifying risks in the use of personal data, legislative advances, and best practices facilitating international cross-border data transfers. It also focused on the impact on Privacy within indigenous groups in various countries and the actions regulators intend to take.

During the closed session, three new

members (Brazil, Niger, and Nigeria) were admitted, expanding membership to regions like Latin America and Africa. Six new observers from international authorities and organizations were also admitted, broadening the perspective to other international rights and concerns.

The triennial Census for 2023 was presented, based on data collected from 78 members, providing accurate and objective information to enhance strategies and the development of future activities within the GPA and among member countries.

Reports from GPA working groups were presented, with highlights including developments by the Digital Economy WG on priority topics such as surveillance technologies, advertising, and web scraping. The Ethics and Data Protection in Artificial Intelligence (AI) WG focused on the use of AI in the workplace and the Generative AI System.

Four workshops led by experts in data protection covered topics like quantum technologies, the metaverse, climate technology, and government digitization. The 2023-2025 strategic plan was presented, and seven resolutions were approved, addressing issues such as artificial intelligence and



employment, health data and scientific research, achieving global standards in data protection, establishing a GPA Library, Generative Artificial Intelligence systems, creating a working group on the intersectional gender perspective in data protection, and the privacy and

human rights award.

It was announced that the Philippines was chosen as the Designated Secretariat, and a transition to a funded secretariat will take place during the coming year.

This year the Giovanni Buttarelli Award was given to Andrea Jelinek and

the Global Privacy Awards were given to the authorities of the BfDI of Germany, INFOEM of Mexico, the Spanish Data Protection Agency of Spain, the INAI of Mexico, the European Data Protection Supervisor and the Hellenic Data Protection Authority. 



GPA

Global Privacy Assembly

globalprivacyassembly.org

 PrivacyAssembly

 privacyassembly